BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 33-202

AIR FORCE MATERIEL COMMAND
Supplement 1

23 MAY 2000

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: http://afmc.wpafb.af.mil.

OPR: AFMC CSO/SCON
(Maj Glenn A. Ratchford)

Certified by: AFMC CSO/SCON
(Col Kevin J. Kirsch)
Pages: 22
Distribution: F

This supplement defines criteria for computer security. Base supplements can add to but not take away from the Air Force Instruction (AFI) and major command supplement. This supplement applies to all AFMC organizations. It also applies to all other organizations and contractors residing on an AFMC base or geographically separated unit (GSU) using computer equipment. It also applies to all organizations connected directly, physically or logically, to the base network.

AFI 33-202, 1 February 1999, is supplemented as follows:

2.6.1. (Added) Form a Systems Security Working Group according to AFI 31-702, *System Security Engineering*, 18 Feb 94, to assist in meeting COMPUSEC requirements. The working group should consist of individuals who are involved in developing software/hardware being installed on the network, and security and security managers.

2.6.2. (Added) Involve the Designated Approving Authority (DAA) and Computer Systems Manager (CSM) early in acquisition and development process.

2.6.3. (Added) Certify and accredit information systems prior to Initial Operating Capability.

2.7.6. (Added) Internet Protocol (IP) addresses shall not be issued until the Wing Information Assurance (IA) office determines that the system has been subjected to the risk management process and is accredited.

2.10.1.8. (Added) Track and maintain all accreditation information and notifies DAAs of reaccreditation due dates no later than six months prior to the reaccreditation date.

2.10.1.9. (Added) The Wing IA office will notify the MAJCOM Information Assurance (IA) office, in writing, of the names, grades, DSN and commercial telephone and FAX numbers, email and mailing address of primary and alternate points of contact. This information shall be updated as soon as any changes occur.

2.10.1.10. (Added) The Wing/Base IA office will provide training to newly assigned unit COMPUSEC managers and hold annual meetings with the managers. The training and meetings shall be documented. The Wing IA office will maintain records of personnel trained, date of training, office, and phone number at a minimum. The Wing IA office shall keep at least the last two years' minutes on hand for review.

2.10.1.11. (Added) Will ensure that a National Security Agency (NSA) approved degausser located on the base is available for their use.

2.11.5. (Added) HQ AFMC and Center staff directorate heads will appoint COMPUSEC managers for their directorates. Appointments will be made in writing to their respective Wing IA offices. The unit COMPUSEC manager and computer system security officer (CSSO) will not be in the MAJCOM or Wing IA office.

3.2.1.3. (Added) Individuals appointed DAA must provide in writing their name, grade, organization/office symbol, DSN and commercial telephone and FAX numbers, email and mailing address to the Wing/Base IA office. This information must be updated immediately upon any change of the submitted information.

3.2.1.4. (Added) Wing/Base IA office will review/update the DAA information at least semi-annually to ensure currency.

3.2.2.3. (Added) HQ AFMC . Authority to approve all AFMC computer systems under their jurisdiction, processing up to and including Top Secret (collateral) information is delegated to each directorate two-letter. They may not delegate their responsibility, but may designate a DAA representative the authority to act in their behalf to attend meetings, gather information, etc.

3.2.4. (Added) DAA for all AFMC systems, processing up to and including Top Secret (collateral) information, is delegated to AFMC center, field operating agency, and direct reporting unit commanders. Commanders may delegate this authority no lower than group commander level in accordance with AFI 33-202. Delegate based on the following guidance:

3.2.4.1. (Added) The delegate will not be part of the IA staff.

3.2.4.2. (Added) The delegate should be in the operational chain of command of the organization for which the system is operating and is most affected by its failure/compromise.

3.2.4.3. (Added) The delegate must ensure that the Wing/Base IA office reviews all certification and accreditation risk analysis packages. Recommendations for approval/disapproval will be provided to the delegate. If recommended for disapproval by the Wing/Base IA, the areas of concern must be fixed and package approved prior to connection and/or operation on the base network. The requester and Wing/Base IA offices will maintain copies and records of package approval/disapproval and recertification required dates.

3.5.1.7.1. (Added) Ensure vendor-produced software/system patches are not implemented unless specified by AFCERT in the form of Compliance/Virus Notification Messages.

3.11.4. (Added) Coordinate the time and duration of the dial-in remote maintenance and administration activities.

3.11.4.1. (Added) The phone line will not be connected to the system except upon coordination and only for the duration of the coordinated and required time to perform remote maintenance/administration.

3.11.4.2. (Added) Disconnect the system being remotely maintained/administrated from the network, as long as disconnection does not unnecessarily impact mission accomplishment.

3.13.3. Viruses transmitted via e-mail Block infected emails and/or attachments at the firewall/base router.

3.13.3.2. (Added) Disconnect external access base e-mail server(s) from any external access until all infected e-mails are deleted from the server(s) and the appropriate anti-virus update software is loaded onto the server(s) and as applicable workstations.

3.13.3.3. (Added) Disconnect all subordinate e-mail server(s) from the base e-mail server until the respective DAA states that their server(s) and workstation(s) are cleaned and the appropriate anti-virus is properly loaded.

3.13.3.4. (Added) Wing/Base IA offices will provide status of efforts to the NOSC once cleanup efforts have terminated.

3.13.3.5. (Added) The CSSO will collect the cleanup costs using the format at attachment 5 and forward the data to the Wing/Base IA office, which in turn will forward this information to the NOSC, as required.

3.13.4.1. (Added) Contact Network Operations and Security Center (NOSC) of any virus attack(s).

3.13.6.1. (Added) The base network control center will automate anti-virus update procedures on all networked computers. The automated tool/script will be configured to not allow user login to the network until the update has been loaded. It will be set up to minimize interaction by the user. At most the user should only need to press enter to reboot.

3.14.1. (Added) All personnel using DoD computer systems or resources will receive COMPUSEC awareness, training, and education at least annually throughout their assignments.

3.14.2. (Added) Use script or other method to automate enforcing personnel to review training material and pass test.

3.14.3. (Added) New personnel must pass the test prior to being allowed to access the network.

3.17. (Added) Vulnerability Assessments AFIWC, the NOSC, and Central Network Control Center (CNCC) are responsible for controlling and performing vulnerability scans. The NOSC and CNCC will have a portable capability, such as, the use of a laptop, so scans can easily be setup in different locations. NOSC and CNCC personnel will ensure they always have the most current version of the vulnerability scan software. The NOSC will query the CNCCs at least every two months or after each release, whichever is shorter.

3.17.2. (Added) The CNCC is the controlling principle for all internal network vulnerability scanning, and testing. For GSUs the controlling Functional/network system administrator will perform the requirements in place of a CNCC.

3.17.3. (Added) Base CNCCs shall utilize Internet Security Scanner (ISS) and/or other approved Air Force scanning tools on at least on a quarterly basis to scan the entire base network for vulnerabilities. The CNCC will ensure all scans are coordinated with the Wing/Base IA office, NOSC and AFIWC. CNCCs will report high-level vulnerabilities and systems associated with those vulnerabilities to the NOSC.

3.17.4. (Added) The CNCC will not publicize scans to the local base populace to ensure the integrity of the data being collected.

3.17.5. (Added) The CNCC will provide the results within 5 workdays to the offending organizations, their CSSO, and functional system administrators for corrective actions.

3.17.6. (Added) The CNCC will correct those vulnerabilities within it's capability, such as forcing users to provide new strong passwords, elimination of default accounts and passwords, etc.

3.17.7. (Added) All high-level vulnerabilities identified by the scan must be eliminated by the system owner within 5 days of notification. CNCCs will notify the NOSC once the vulnerabilities have been closed.

3.17.8. (Added) The CNCC will run a follow-up scan as required to check status. Unless proper justification is provided for not eliminating the vulnerabilities, those accounts, computers, or subnets will be disabled or disconnected from the base network until properly resolved.

3.17.9. (Added) The MAJCOM NOSC will perform external scans on base networks using ISS and/or other approved Air Force scanning tools. The results will be forwarded to the respective CNCC/GSU with directions and timelines to eliminate identified vulnerabilities.

3.17.10. (Added) The MAJCOM NOSC will coordinate the scans with the appropriate organizations to include the base CNCC or GSU functional/network administrator.

3.17.11. (Added) The Wing/MAJCOM IA office will request specific actions taken regarding systems that are exploited via on-line surveys in accordance with the table at attachment 2. Wing/Base DAA, IA, and CNCC will ensure all required actions are completed to meet the MAJCOM suspense dates.

3.17.12. (Added) Any unauthorized contractor, military, or government personnel that attempt to perform unauthorized scans, password cracking, etc., may be subject to criminal/UCMJ proceedings. Actions taken will be determined by the local JA and OSI.

3.18. (Added) Remnance Security Classified Information on Unclassified Computers and/or Transmitted Unencrypted Via Unclassified Network Services

3.18.2. (Added) Report classified information on computer(s) or transmitted unencrypted via unclassified network services such as e-mail and web sites to the unit CSSO. (see attachment 6)

3.18.3. (Added) The CSSO will

3.18.3.1. (Added) Notify base security forces, base DAA, wing information assurance personnel, and unit security manager.

3.18.3.2. (Added) Provide the Wing/Base IA office the name, phone number, e-mail address, and base of the originator.

3.18.3.3. (Added) Inform the Wing/Base IA office if personnel in their office forwarded or sent the e-mail to other personnel. If so the CSSO will provide the Wing/Base IA office a list of names, phone numbers, and e-mail addresses listed by base.

3.18.3.4. (Added) The CSSO and/or the reporting individual will contact the originator to inform them of the problem and actions the originator needs to take to report the incident, which include contacting their CSSO, base network control center (NCC), Wing/Base IA office and security forces personnel.

3.18.4. (Added) Wing/Base IA will

3.18.4.1. (Added) Contact Security forces, coordinate efforts, and share information to ensure the clean up of the classified information. Wing/Base IA personnel will immediately notify MAJCOM Information

Assurance (IA) Office for a control number to track the incident. The two-ltr organization responsible for the incident will complete the incident report in accordance with AFSSI 5021, *Vulnerability and Incident Reporting* and forward the report to the Wing/Base IA office. The Wing/Base IA office will then forward the report MAJCOM IA office.

3.18.4.2. (Added) Ensure the MAJCOM NOSC is kept updated on status and actions as required by the NOSC.

3.18.4.3. (Added) Ensure the NCC is promptly notified so they can take actions to block, eradicate and take other appropriate actions as required. Use attachment 7 as a checklist to clean the file(s).

3.18.4.4. (Added) Track, monitor, guide, and report file/e-mail removal efforts.

3.18.4.5. (Added) Ensure the e-mail is blocked, by subject, at the firewall/base router from entering or leaving the base.

3.18.4.6. (Added) Ensure the CSSO, originator, and/or any personnel who sent the e-mail out to others, contact the recipients of the e-mail. This pertains only to those organizations that their personnel sent the e-mail to others.

3.18.4.7. (Added) CSSO will collect cleanup costs to include man-hours expended, hardware, and software. Provide this in excel in the format at attachment 5, to the Wing/Base IA office or as required by the NOSC.

3.18.5. (Added) The NOSC will

3.18.5.1. (Added) Contact all AFMC bases/units impacted as well as all other NOSCs whose bases are impacted by the incident.

3.18.5.2. (Added) Coordinate and track efforts to block further dissemination and to eradicate the file(s) and e-mail(s) within AFMC.

3.18.5.3. (Added) Ensure all AFMC units block the e-mail by subject at the firewall/base router.

3.18.5.4. (Added) Inform all AFMC bases of completion of clean up efforts.

3.18.5.5. (Added) Keep HQ AFMC/SC updated on efforts and actions taken.

3.18.5.6. (Added) Consolidate cleanup costs and provide to AFMC/SC to decide reimbursement from the originator's organization/Command.

3.19. (Added) Web Services Public access and restricted access web sites will not reside on the same server.

3.19.2. (Added) Only public access web sites may be on public access servers. Public access web servers will be located outside the base firewall.

3.19.3. (Added) Any server with restricted access web sites will be set up to allow only .mil/ access and will be located inside the base firewall.

3.19.4. (Added) A process for evaluating and ensuring all information is appropriate and publicly releasable should be obtained through Public Affairs and adhered to by personnel posting information to public web sites.

3.19.4.1. (Added) No information will be posted on public access web servers without the review and approval of Public Affairs.

3.19.4.2. (Added) GSUs and wings will review in detail the public access web sites at their base/locations. The center and wing may combine into one cross-functional review board to review all the public access web sites from the center level and below. If not, the center will review in detail their public access web sites and perform a random review of the wing level public access web sites.

3.19.4.2.1. (Added) Cross-functional review boards will, at a minimum, consist of representatives from the Public Affairs, Communications, Legal, Contracting, Security Forces, Intel, Air Force Research Laboratory/Site personnel (where applicable), and Operations. The board may include any other representatives necessary to address questions concerning the sensitivity of information on a public web site.

3.19.4.3. (Added) Releasing authorities for the information will review publicly accessible web sites at least annually to ensure that sensitive information (acquisition, technology, privacy, legal, security, etc) does not appear on the public web site.

3.19.4.4. (Added) The review boards and/or users of a web site who believe that information in compilation or aggregation on a system or systems to which they have access contains classified information, should contact the webmaster of the system(s) in question or, if the webmaster is unknown, report the matter to their own organization's security office for evaluation and action as appropriate. Use the excerpt at attachment 8 (see AFI 33-129, *Transmission of Information via the Internet*, 1 Aug 99, for additional guidance).

3.19.5. (Added) Publicly accessible DoD web sites will not normally contain links or references to DoD web sites with security and access controls. Under certain circumstances, however, it may be appropriate to establish a link to a log-on site provided details as to the controlled site’s contents are not revealed.

3.20. (Added) E-mail Security: E-mail will not be automatically forwarded to non-military/government e-mail addresses.

3.20.2. (Added) The use of automatically forwarding e-mails to non-military/government e-mail addresses should be strongly discouraged to avoid the transmitting of sensitive information. Educate users of the dangers of automatically forwarding e-mails to non-military/government e-mail addresses.

3.20.3. (Added) Personnel who want to access their work e-mail while TDY or on leave must use an authorized remote access server dial-up capability to access their military/government e-mail.

3.20.4. (Added) Personnel will not TELNET into any base or government network from a non-.mil/.gov site/network. If TELNETing is a must, adhere to AFSSI 5027 paragraph 6.15.3 guidance.

3.20.5. (Added) Never open attached files with extensions of .exe, .bat, .com, until verified with the sender that the file is valid and does not contain malicious logic.

3.20.6. (Added) When Public Keying Infrastructure (PKI) certificates have been issued, all e-mail transmissions to personnel on military and/or government networks must be digitally signed using the PKI certificates.

3.20.6.1. (Added) A PKI enabled user who receives an e-mail from another PKI enabled user should not open the e-mail (including attachments) unless it has been digitally signed.

3.20.7. (Added) Out-of-office response mailing guidance. It is strongly recommended that management consider the risk of using out-of-office response mailing. Because the user indicates what information is sent in the response, care must be taken that OPSEC is not violated.

3.20.7.1. (Added) If used, do not include purpose of absence, location, or other potential OPSEC information.

3.20.7.2. (Added) If the absence will be greater than two weeks, do not include the return date.

3.20.7.3. (Added) Information to include is who may be contacted during your absence and their phone number.

3.21. (Added) Policy Compliance Violations CNCC/Wing IA personnel will review “profiler” or any follow-on software as needed.

3.21.1.1. (Added) Analysis will be performed on the data and actions taken to ensure unauthorized, high bandwidth sites are blocked at the firewall and/or router.

3.21.1.2. (Added) Any extended/repeat visits to or downloading of material from unauthorized sites by individuals will be reported through the Comm Squadron Commander to the wing base network DAA and to the organization of the offending individual(s) for proper action (attachment 2). The report will be via a formal memo (example at attachment 3) to the offender’s organization.

3.21.1.2.1. (Added) Depending upon severity of the violation will determine if individuals accounts are disabled until a memo from the individuals organization stating the person has satisfactorily completed remedial computer and network training and should be allowed access to the network (example at attachment 4). Use the table at attachment 2 as a guide to determine when to disable an individual’s account upon approval to do so from the base network DAA.

3.21.2. (Added) Wing/Base IA will maintain copies of all network and standalone System Security Authorization Agreements (SSAAs). This information will be maintained in a database for ease of use and to track required recertification dates.

3.21.2.1. (Added) The CNCC will logically and/or physically disconnect from the base network any subnet or computer that does not have a full or interim DAA approved by the base network DAA.

3.21.2.2. (Added) The using organization must complete the documentation and get their DAA’s approval to operate the LAN while not connected to the base network. IAW AFI 33-115 V1, para 6.4.3.1.1.

3.21.2.3. (Added) If the organization requires their computer(s) and/or LAN to be connected to the base network, the requiring organization must provide the certification and accreditation package and SSAA to the base network DAA for review and approval to connect and operate on the base network.

3.21.2.4. (Added) The Wing/Base IA will maintain records of the approval date and send a reminder to the organization at least six months prior to expiration date.

3.21.2.5. (Added) If the organization has not completed recertification by the expiration date, the CNCC will disconnect the subnet(s)/computer(s) from the base network. IAW AFI 33-115 V1, para 6.4.3.4.2.

3.21.2.6. (Added) All external network connection requirements must be reviewed, coordinated, provided a solution, and approved by the CNCC.

3.21.2.7. (Added) Any external unauthorized connection to LAN or computers connected to the base network will either be disconnected or result in the disconnection of the offending subnet(s) and/or computer(s). IAW AFI 33-115, para 6.4.3.1.1 and para 6.4.3.4.2.

3.22. (Added) Network Access, Login, and Password Management If commercially available, must purchase, install, and implement automated tool to enforce strong password generation. Set automated tool to ensure passwords include characters from all four character set groups (upper case letters, lower case letters, numbers, and special characters i.e. ? / %). The product for Windows NT servers is the NT resource kit.

3.22.2. (Added) Users will activate password protected screen savers any time they leave their workstation unattended. All systems will be configured to provide the ability to activate password protected screensavers.

3.22.3. (Added) During elevated Information Conditions (INFOCONs) abide by appropriate INFOCON requirements for duration of passwords and other password change requirements.

3.22.4. (Added) System administrator default accounts will be disabled after building a mandatory alternate system administrator account.

3.22.4.1. (Added) The new account will not use any portion of the title system administrator.

3.22.4.2. (Added) The system administrator account will be a combination of the administrator's first name, last name, and or middle name. However, it must not be the same as the administrator's network user account login nor will it include a number. (example: User/administrator David Allen Jones - user login - jonesd; sys admin login - jonesda)

3.22.4.3. (Added) Passwords will be changed at intervals not to exceed 90 days.

3.22.4.4. (Added) User's remote access server (RAS) dial-up access login must be different than any other login to base resources/network. (example same as 3.22.4.2.)

3.22.4.5. (Added) Passwords for RAS, system administration, and user accounts must all be different. No two for an individual user may be the same.

3.22.5. (Added) Users will log off/turn off their computers at the end of each workday, unless the NCC requests otherwise.

3.22.6. (Added) Where possible ensure network automatically disconnects a user if more than three hours inactivity during non-duty hours. During duty hours allow no more than eight hours of inactivity.

3.23. (Added) Account Management Ensure controls are in place to monitor the use and provide timely removal (within 3 days) of user accounts from the system or network, when necessary (e.g., disgruntled employee, change in contractors, inactive account, etc.).

3.23.2. (Added) Ensure controls are in place to ensure notification and remarks are added to a users account identifying dates of extended periods when a user will not access their account due to leave or TDYs 30 days or longer. The account will be disabled until the user returns and requests account activation. If no updates are provided for the account, and it is more than 60 days past expected return date. Notify the responsible CSSO to determine if account should be deleted or if person is on extended leave/TDY.

3.24. (Added) IP Address Management Use of Dynamic Host Configuration Protocol (DHCP)

3.24.2. (Added) It is recommended to use static IP addresses to allow for non-repudiation and security purposes

3.24.3. (Added) Logs must be able to be read without interrupting current network operations.

3.24.4. (Added) Logs must contain sufficient historical data to correlate IP addresses with specific devices. Logs must be maintained for at least 90 days.

3.24.5. (Added) Internal nodes will use private IP addresses. Use the 172.0.0.0 and the 10.0.0.0 range for those nodes that do not require direct external access. Only external access computers and equipment such as servers will use routable IP addresses, all others will comply with the Barrier Reef concept to conceal the network.

Attachment 1 (ADDED)
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

(Added) AFI 33-129, Transmission of Information via the Internet, 1 Aug 99

Attachment 2 (ADDED)

POLICY VIOLATION DECISION TABLE OFFENSES WITHIN A 6-MONTH PERIOD

	1st Offense	2nd Offense	3rd Offense	>3 Offenses
Incorrect use of authorized modem on PC connected to base network (concurrent network and modem connection)	Memo to organization reminding them of the proper procedures for use	Disable individual's account and block that IP from the network	Memo to organization requiring individual and organizational commander explain in person to wing or center commander that the individual will not have any more violations within the six month period and why the individual should be allowed access to the network	Same as 3rd offense, with consideration to not allowing individual access to the base network for an extended or indefinite period of time.
Password cracked due to weak or non compliant password	Force password change upon next login. Inform individual via e-mail that account will be disabled upon next time password is cracked.	Memo to organization informing them of policy. Disable the individual's account. Force password change upon next login.	Memo to organization requiring individual and organizational commander explain in person to wing or center commander that the individual will not have any more violations within the six month period and why the individual should be allowed access to the network	Same as 3rd offense, with consideration to not allowing individual access to the base network for an extended or indefinite period of time.

Adding unauthorized external connection to PC or subnet connected to the base network	Disconnect at the appropriate level the circuit/subnet/ PC. Send memo to organization of violation.	Disconnect at the appropriate level the circuit/subnet/PC. Send memo to organization of violation.	Disconnect at the appropriate level the circuit/subnet/ PC. Send memo to organization of violation requiring the offender and the organization commander in person explanation.	Same as 3rd offense, with consideration to not allowing individual/organization access to the base network for an extended or indefinite period of time.
Sending classified over the unclassified network	Disable users account. Send memo to organization of violation.	Disable users account. Send memo to organization of violation requiring the offender and the organization commander in person explanation.	Same as 2nd offense, with consideration to not allowing individual access to the base network for an extended or indefinite period of time.	Same as 3rd offense, do not allow individual access to the base network for at least 30 days or an indefinite period of time.
Using streaming audio or video for other than mission related requirements, i.e. listening to radio station over the network, sports casts, etc.	Disable users account. Send memo to organization of violation.	Disable users account. Send memo to organization of violation requiring the offender and the organization commander in person explanation.	Disable users account. Send memo to organization of violation requiring the offender and the organization commander in person explanation.	Same as 3rd offense, with consideration to not allowing individual/organization access to the base network for an extended or indefinite period of time.
Extended (over 1 minute at one site) visits/ repeat visits to the same site/ downloading pornographic material from the internet	Disable users account. Send memo to organization of violation requiring the offender and the organization commander in person explanation. Consider contacting OSI to determine if they need to investigate the incident.	Disable users account. Send memo to organization of violation requiring the offender and the organization commander in person explanation. Contact OSI to determine if they need to investigate the incident.	Disable users account for at least 30 days. Send memo to organization of violation requiring the offender and the organization commander in person explanation. Contact OSI to investigate the incident.	Permanently delete the users account. Send memo to organization of violation informing the offender and the organization commander of the action.

Attachment 3 (ADDED)
EXAMPLE MEMORANDUM
OF

POLICY VIOLATION NOTIFICATION

MEMORANDUM FOR 557 ABW/DO

FROM 557 ABW/CC

SUBJECT: 1ST Policy Violation by *Name of offending individual, office symbol*

1. *Name of offender, office symbol* has violated network policy by *specify offense* (example, downloading files from an unauthorized pornographic site, or installing an unauthorized modem on networked computer, sending classified material over the unclassified network).

2. Please ensure the individual receives computer and network remedial training to preclude future violations.

3. (Optional paragraph dependent on whether or not individual's account was disabled) *Name of offender's* network account has been disabled until we receive a memo (example at attachment 2) signed by the organizational commander requesting the account be enabled and stating the individual has successfully completed computer and network remedial training.

Attachment 4 (ADDED)
EXAMPLE MEMORANDUM REPLY
REQUESTING INDIVIDUAL'S ACCOUNT REACTIVATION

MEMORANDUM FOR 557 ABW/CC
557 ABW/CS
IN TURN

FROM 557 ABW/DO

SUBJECT: Recertification of *offender*'s *name*, *office symbol, phone number*

1. *Offender's name* has successfully completed computer and network remedial training. He/she has been informed of potential consequences of repeat computer and network policy violation. Access to the network is mission required. Request his/her network account be enabled.

2. Please contact *offender's name* upon approval and activation of his/her network account.

3. If you have any questions, please contact our computer system security officer *name, phone number*.

Attachment 5 (ADDED)
INCIDENT COSTS INCIDENT/VIRUS "NUMBER/NAME" BASE

Filename convention is: base incident number/virus name.xls use either the incident number or the virus name depending on if it is a classified incident or a virus cleanup actions.

Man hours						
Contractor Regular	Contractor Overtime	DoD Civilian	Military	Hardware Costs	Software Costs	Misc. Costs

Attachment 6 (ADDED)

REMNANCE SECURITY REPORTING

A6.1. Base Security Forces POC (name, rank, phone number, e-mail address:

A6.2. Incident number:

A6.3. Reporting User (the user who reported finding the classified information), (name, rank, phone number, e-mail address):

A6.4. Reporting CSSO (the CSSO in the organization that reported the incident), (name, rank, phone number, e-mail address):

A6.5. Originator of e-mail (name, rank, phone number, e-mail address, base/site location):

A6.6. E-mail subject line (the exact subject title/wording on the e-mail subject line):

A6.7. List of addressees by base that user/originator sent the e-mail (only those sites that the user has sent the e-mail to others need to provide this information):

Attachment 7 (ADDED)
REMNANCE SECURITY CLEANUP CHECKLIST

- ❑ Identify all alias file names

- ❑ Identify all Storage locations
  - ❑ Local Drives
  - ❑ Network drives
  - ❑ Removable media
  - ❑ Backup Tape
  - ❑ Floppy Disk
  - ❑ Zip Disk
  - ❑ Jazz Disk
  - ❑ CD-R(or RW
  - ❑ Other

- ❑ Get Incident number from Security Forces/NOSC

- ❑ Contact and report information to NOSC

- ❑ Identify all recipients e-mail forwarded/sent
  - ❑ In-house/base network
  - ❑ Other Government Organizations
  - ❑ Commercial/Industry Organizations
  - ❑ Academic Organizations
  - ❑ Other

- ❑ Clean Recipient's workstation(s) on base
  - ❑ Delete/Wipe files
  - ❑ Wipe free space

- ❑ Collect and control all affected removable media with safeguards to level of classification required by the information
  - ❑ Clean/wipe Removable media
    - ❑ Delete/wipe file
    - ❑ Wipe Free Space
  - ❑ Degauss Media
  - ❑ Destroy Media

Attachment 8 (ADDED)

EXCERPT FROM WEB SITE POLICY GUIDE FOR IDENTIFYING INFORMATION INAPPROPRIATE FOR POSTING TO A PUBLICLY ACCESSIBLE DOD WEB SITE

This guidance is authorized to be used for one purpose only: identifying information that may be inappropriate for posting to publicly accessible DoD web sites. **It is not to be used as guidance in responding to requests under the FOIA or the Privacy Act under any circumstances.** It is intended as an interim guide to the identification of categories of information that are inappropriate for posting to a publicly accessible web site. Additional guidance will be forthcoming when this document is formalized in the DoD publication system.

FOR OFFICIAL USE ONLY (FOUO) information may not be posed to official web sites that are open to public access. (Information which is typically FOUO is followed by an * below). Also identified below is information whose sensitivity may be increased when electronically aggregated in significant volume. All information proposed for posting to a publicly accessible web site must be reviewed in accordance with the provisions of DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)) and as described in Paragraph 3, Part II of this document.

Do not use this compendium as the sole source for identifying such information. Questions about FOUO information should be referred to your local FOIA office. Questions about aggregated information should be referred to your local security office and/or OPSEC coordinator.

A8.1. Military Operations & Exercises information relating to:

- Unit Organization
- Unit readiness specificity
- Detailed mission statement should be approved by PA
- Specific Unit phone/fax numbers (secure and unsecured)
- Time-Phase Force Deployment Data (TPFDD)
- Ops schedules
- Logistics support requirements
  - Medical
  - Civil engineering
  - POL
  - Host nation support
  - Transportation
  - Munitions
- Force Apportionment
- Force Allocation
- Unit Beddown information
- Planning guidance

- Unit augmentation
- Force Synchronization
  - Unit shortfalls
- Counterterrorism information
- Detailed Budget Reports
- Images of Command and Control (C2) nodes
- Inventory reports
- Operational Readiness Inspection Reports (or reports that reveal mission vulnerabilities)
- Intelligence, Surveillance and Reconnaissance (ISR) Capabilities
- Command, Control, Communications, Computers and Intelligence(C4I) Architecture
- Noncombatant Evacuation Operations (NEO) Plans or Ops
- Counter-drugs Ops
- Unit Recall Rosters
- Weapons Movements
- Mobilization information
- Detailed maps or installation photography
- Standard Operating Procedures
- Tactics, Techniques, and Procedures
- Critical maintenance

A8.2. Personnel information relating to:

- Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: (1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty phone numbers of units described in C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.*
- Names, locations, and any other identifying information about family members of DoD employees and military personnel*
- Official travel itineraries of individuals and units before it is performed*
- Duty rosters, or detailed organizational charts and directories with names (as opposed to organizational charts, directories, general telephone numbers for commonly requested resources, services and contacts without names)*
- Internal DoD personnel rules and practices unless cleared for release to the public*
- Financial Disclosure Reports of Special Government Employees (5 USC App. 4, ß207 (a) (1) 2)*
- Representation Rights and Duties, Labor Unions (5 USC ß7114 (b)(4))*
- Action on reports of Selection Boards (10 USC ß618)*
- Confidential Medical Records (10 USC ß1102)*
- Civil Service Examination (18 USC ß1917)*

- Drug Abuse Prevention/Rehabilitation Records (21 USC ß1175)*
- Confidential of Patient Records (42 USC ß290dd-2)*
- Information Concerning US Personnel Classified as POW/MIA During Vietnam Conflict (42 USC ß401)*
- Information Identifying Employees of DIA, NRO, and NIMA (10 USC ß424)*

A8.3. Proprietary Information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public. Other specific provisions include:

- Contractor Proposals (10 USC ß2305 (g))*
- Commercial or financial information received in confidence with loans, bids, contracts or proposals*
- Information received in confidence e.g. trade secrets, inventions, discoveries or other proprietary data*
- Statistical data and commercial or financial information concerning contract performance, income, profits, losses and expenditures, if offered and received in confidence from a contractor or potential contractor*
- Scientific and manufacturing processes or developments concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress*
- Test and evaluation of commercial products or military hardware produced by a nongovernmental entity*
- Patents, unless licensed for publication by the United States*
- Software documentation: shall be distributed according to the terms of the software license*
- Premature Dissemination: The information related to patentable military systems or processes in the developmental stage.*
    - Confidential Status of Patent Applications (35 USC ß 122)*
    - Secrecy of Certain Inventions and Withholding of Patents (35 USC ß181-188)*
    - Confidential Inventions Information (35 USC ß205)*

A8.4. Test and Evaluation information could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations, or incapabilities of a DoD weapons systems or component.

A8.5. Scientific and technological information relating to:

- Critical technology on either the Munitions List or the Commerce Control List*
- Unclassified Special Nuclear Weapons Information (10 USC ß128)*
- Unclassified Technical Data with Military or Space Application (10 USC ß130)*
- Centers for Industrial Technology – Reports of Technology Innovations (15 USC ß3705 (e)(E))*
- Information Regarding Atomic Energy (42 USC ß2161-2168)*
- Control of Arms Exports Sec 38(e) of the Arms Export Control Act (22 USC ß2778(e))*

- Technical and scientific data developed by a contractor or sub-contractor exclusively or in part at private expense*
- Sensitive S&T Reports such as:*
    - Defense Acquisition Executive System Reports
    - Selected Acquisition Reports
    - Weapons System Unit Cost Reports
    - Approved Program Baselines for ACAT I, II, III Weapons Systems
    - Weapon Systems Evaluation and Testing Results and Reports
    - Reports Based on Joint USA and Foreign Government Technical Research and Weapons Systems Evaluations
    - Weapons System Contractor Performance Reporting Under earned Value Reporting System at the Level of CPE Reporting
    - Weapons Systems staff working papers, correspondence and staff assessment
    - DoD Component "Feedback" staff working papers and assessments on weapons System Program Performance

A8.6. Intelligence information relating to:

- Organizational & Personnel Information for DIA, NRO and NIMA (10 USC ß424)*
- Maps, Charts, and Geodetic Data (10 USC ß455)*
- Communications Intelligence (18 USC ß798)*
- NSA Functions and Information (50 USC ß402)*
- Protection of Identities of US Undercover Intelligence Officers, Agents, Informants and Sources (50 USC ß421)*
- Protection of Intelligence Sources and Methods 50 USC ß403(d)(3))*

A8.7. Other information relating to:

- A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations
- Administrative Dispute Resolutions (5 USC ß574 (j))*
- Confidentiality of Financial records (12 USC ß3403)*
- National Historic Preservation (16 USC ß470w-3)*
- Internal advice, recommendations and subjective evaluations*

DEBRA L. HALEY, SES
Director, Communications and Information